News Release

報道各位

2022 年 12 月 20 日
トビラシステムズ株式会社

トビラシステムズ、2022 年のスミッシングトレンドワードと手口ランキングを発表
～スミッシング件数は前年比約 2 倍、通信事業者や国税庁を装う手口が増加～

トビラシステムズ株式会社（本社：愛知県名古屋市、代表取締役社長：明田 篤、証券コード：4441、以下「トビラシステムズ」）は、独自の迷惑情報データベースをもとに調査し集計した「スミッシングトレンドワード 2022」を発表いたします。また、スミッシングで多かった手口のランキングも発表しました。2021 年に比べ、2022 年はスミッシングの件数が約 2 倍に増加しており、通信事業者や、国税庁などの公的機関を装う手口が増加していることがわかりました。

■スミッシングトレンドワード 2022

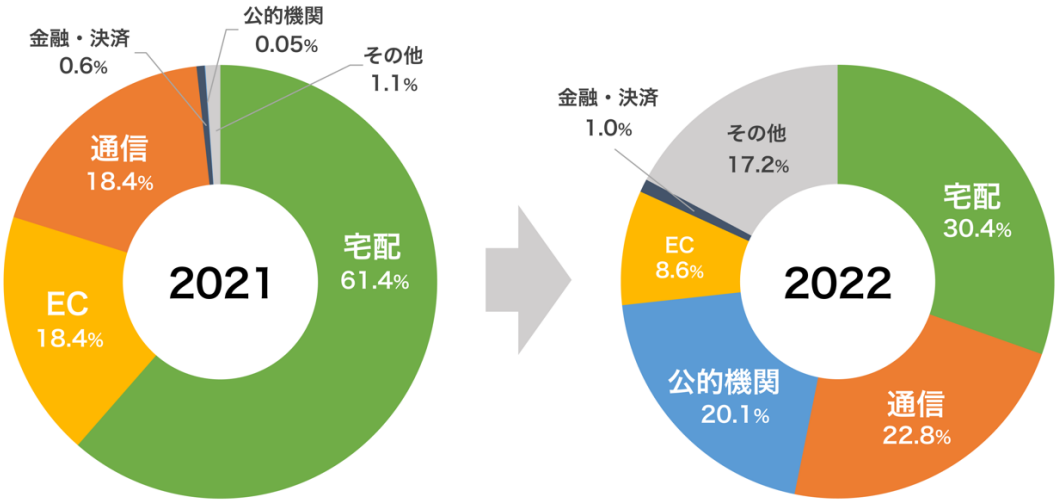
今回のワードマップに登場する単語は、トビラシステムズの調査において、2022 年にスミッシングの文面で頻出した単語です。文面に多く使われた単語ほど、大きく表示されています。ワードマップを参考に、防犯にお役立てください。

■2022 年のスミッシング概況と前年からの変化

当社の調査で、2022 年 1 月～11 月に確認されたスミッシングの件数は、前年同期比で約 2 倍に増加しています。

当社の調査では、2022 年は宅配便の不在通知を装うスミッシング手口の割合が最も多く、昨年に引き続き 1 位でした。ネット通販サイトなどの EC 事業者を装う手口は、全体に占める割合が昨年に比べ減少しました。一方で、通信事業者、公的機関を装う手口の割合が増加し、上位となりました。

スミッシング手口の変化



（トビラシステムズ調べ）

スミッシング手口ランキング

順位	2021	2022	昨年比順位
1	宅配	宅配	→
2	EC	通信	↑
3	通信	公的機関	↑
4	金融・決済	EC	↓
5	公的機関	金融・決済	↓

（トビラシステムズ調べ）

（参考）スミッシングトレンドワード 2021
https://tobila.com/news/release/p1141/

■2022 年のスミッシング三大手口

トビラシステムズの調査で確認された、2022 年に発生したスミッシングで特に多かった 3 つの手口について解説します。

1 位：宅配便の不在通知を装う手口

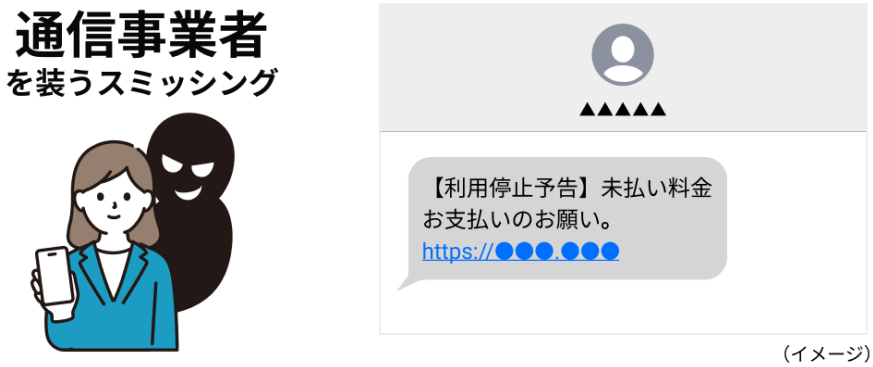
宅配便の不在通知を装う手口が、2021 年に引き続き、最も多く確認されました。なお、2021 年は SMS の文面上で大手宅配事業者の会社名を悪用する手口が多い傾向でしたが、2022 年は特定の会社名を入れず、より汎用的な宅配便の不在通知に見える文面を使用する手口がトレンドでした。コロナ禍で新たにネット通販や宅配サービスを利用する人が増えた中、引き続き注意が必要です。

また、年末年始は、お歳暮や贈り物、ネット通販のおせち料理や福袋など、配達物を受け取る機会が増えます。年末年始も油断せず、宅配便の不在通知を装うスミッシングに注意してください。

（イメージ）

2 位：通信事業者を装う手口

昨年から目立ち始めた通信事業者を装うスミッシングが、2022 年に入り一段と増加しました。利用料金の支払いやアカウント不正利用などの緊急を装う内容で、偽サイトの URL をクリックさせます。偽サイトで個人情報を盗み取る他、通信事業者が提供するセキュリティアプリに似せた偽アプリ（マルウェア）をインストールするよう誘導し、被害者の端末を感染させ、被害をさらに拡大させる手口も見られました。国内の大手通信事業者の名前を騙るため、スマートフォンや携帯電話を持つ人なら誰もが騙されてしまう危険性が潜んでいます。



（イメージ）

3 位：官公庁など公的機関を装う手口

官公庁などの公的機関を装うスミッシングが新たなトレンドとして観測されました。コロナウイルスに関連した助成金の案内を装い厚生労働省の偽サイトに誘導する手口や、国税庁や警察庁を装う手口が見られました。中でも、2022 年 8 月ごろから国税庁を装うスミッシングが顕著に増加しています。国税庁の偽サイトで個人情報を盗み取るケースや、プリペイドサービスを利用し架空料金を支払わせるケースも見られました。

（イメージ）

当社調査で確認されたその他のスミッシング手口の中には、昨今の時勢に便乗するものも見られました。コロナ禍に便乗し、ワクチン接種や助成金に関する内容のスミッシングが昨年に引き続き発生しています。また、コロナ禍で旅行や遠出を自粛する人もいる状況下で、交通系サービスの自動退会手続きを装い、偽サイトに誘導する手口が散見されました。昨今のウクライナ情勢に便乗し、仮想通貨で義援金を募る不審なサイトに誘導する手口も発生しました。その他、スミッシングの文面で悪用された仮想通貨関連のワード（仮想通貨取引所やウォレット等）は、2021 年の 2 種類から 2022 年は 11 種類に増加しました。

なお、スミッシングの手口は日々変化しています。ワードマップに登場した単語や手口のランキングに関わらず、身に覚えのない不審な SMS を受け取った場合は、文面に添付された URL にアクセスしないようご注意ください。

よく利用するサービスの名前で SMS が届いた場合も、文面に添付された URL から直接アクセスするのを避け、公式アプリやあらかじめブックマークした公式サイトを利用するよう心がけてください。

日頃の対策だけでは完全に防ぎきれないケースに備え、迷惑 SMS 対策サービスも併せてご活用ください。

■トビラシステムズの迷惑 SMS 対策サービス

トビラシステムズでは、迷惑電話番号や迷惑 URL、詐欺 SMS の文面パターン等を日々データベース化し、迷惑な SMS の受信時に自動で迷惑メッセージフォルダ振り分けや警告表示を行う迷惑 SMS 対策サービスを提供しています。当社の迷惑情報データベースを使用したモバイル向け各種迷惑情報フィルタサービスを、スミッシング対策にぜひご活用ください。

モバイル向けサービス一覧
https://tobilaphone.com/mobile/

■スミッシングとは

実在する企業やブランドを騙る SMS やメールを送り、添付された URL にアクセスさせて偽サイトに誘導し、個人情報を盗み取る犯罪をフィッシング詐欺といいます。スミッシングとは「SMS」と「フィッシング」を組み合わせた造語で、フィッシング詐欺の中でも SMS を用いたものを指します。

スミッシングの中には、個人情報の詐取以外に、URL 遷移先から悪意のあるソフトウェア（マルウェア）をインストールさせ、マルウェアに感染した端末からフィッシング SMS を大量送信させるよう遠隔操作する手口もあり、被害拡大の一因となっています。

■「スミッシングトレンドワード」とは

トビラシステムズの迷惑情報データベース内で確認された、スミッシングで使用された特徴的なワードを抽出し、使用頻度に応じた大きさで表現したワードマップです。

（参考）スミッシングトレンドワード 2021
https://tobila.com/news/release/p1141/

■トビラシステムズについて

テクノロジーで社会課題の解決を目指し、特殊詐欺やフィッシング詐欺、水面下で発生する迷惑行為「グレーゾーン犯罪」撲滅のため様々なサービスを提供しています。迷惑電話やフィッシング詐欺に関する情報を収集してデータベースを構築し、危険な電話や SMS を自動でフィルタリングする主力事業の「迷惑情報フィルタサービス」は、固定電話、モバイル、ビジネス向けに展開し月間 1,500 万人以上にご利用いただいています。

■本件に関する報道関係のお問い合わせ先

トビラシステムズ株式会社
〒460-0003 愛知県名古屋市中区錦 2 丁目 5-12 パシフィックスクエア名古屋錦 7 F
担当：営業企画部 広報主任 岩渕
TEL：050-3646-6670（直通）
FAX：052-253-7692
URL：https://tobila.com/